WX6103与iMC+Drcom配合实现Portal认证功能的典型配置

任立波 2008-09-08 发表

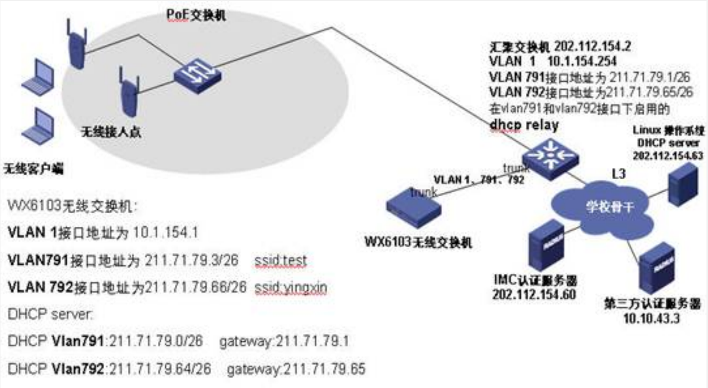
WX6103与iMC+Drcom配合实现Portal认证功能的典型配置

适用与WX6103版本: Comware Software, Version 5.20, Release 2107

一、组网需求:

WX6103、WA2220、H3CPOE交换机、便携机（安装有11b/g无线网卡）、IMC服务器、CAMS服务器、DHCP服务器、汇聚交换机。

二、应用组网图:


PoE交换机
无线接入点
无线客户端
汇聚交换机 202.112.154.2
VLAN 1 10.1.154.254
VLAN 791接口地址为 211.71.79.1/26
VLAN 792接口地址为211.71.79.65/26
在vlan791和vlan792接口下启用的
dhcp relay
Linux 操作系统
DHCP server
202.112.154.63
trunk
L3
VLAN 1、791、792
trunk
学校骨干
WX6103无线交换机
IMC认证服务器
202.112.154.60
第三方认证服务器
10.10.43.3
WX6103无线交换机:
VLAN 1接口地址为 10.1.154.1
VLAN791接口地址为 211.71.79.3/26 ssid:test
VLAN 792接口地址为211.71.79.66/26 ssid:yingxin
DHCP server:
DHCP Vlan791:211.71.79.0/26 gateway:211.71.79.1
DHCP Vlan792:211.71.79.64/26 gateway:211.71.79.65

无线客户端接入SSID:test属于VLAN 791,网关在汇聚交换机上为211.71.79.1。 无线客户端接入SSID:yingxin为VLAN792,网关在汇聚交换机上为211.71.79.65

IMC服务器地址：202.112.154.60（做portal server 和第二个radius server)

第三方服务器地址为：10.10.43.3（第一个radius server)

注意：保证WX6103到IMC、第三方radius服务器路由可达，且注意中间无防火墙将对应端口封堵，此典型配置为实际校园组网，为满足SSID:test用户可以访问校园内外网，SSID：yingxin用户只能访问校内网。

三、WX6103的典型配置

```
 version 5.20, Release 2107
#
 sysname WX6103
#
 domain default enable bjtu
#
 telnet server enable
#
 portal server h3c ip 202.112.154.60 key h3c url http://202.112.154.60:8080/portal
 portal free-rule 0 source any destination ip 211.71.79.0 mask 255.255.255.192
 portal free-rule 1 source any destination ip 211.71.79.64 mask 255.255.255.192
 portal free-rule 3 source any destination ip 202.112.144.236 mask 255.255.255.255
 portal free-rule 4 source any destination ip 202.112.144.246 mask 255.255.255.255
 portal free-rule 5 source ip 202.112.144.236 mask 255.255.255.255 destination any
 portal free-rule 6 source ip 202.112.144.246 mask 255.255.255.255 destination any
#
 user-isolation vlan 1 enable
 user-isolation vlan 1 permit-mac 000E-84FA-4C80 000F-E290-A942
#
vlan 1
#
vlan 791 to 792
#
radius scheme bjtu
 primary authentication 10.10.43.3
 key authentication wireles
 user-name-format without-domain
 nas-ip 10.1.154.1
radius scheme h3c
 primary authentication 202.112.154.60
 primary accounting 202.112.154.60
 key authentication h3cwireless
 key accounting h3cwireless
 nas-ip 10.1.154.1
radius scheme wang
 primary authentication 127.0.0.1
 primary accounting 127.0.0.1
 key authentication wang
 key accounting wang
 nas-ip 172.0.0.1
#
domain bjtu
 authentication portal radius-scheme bjtu
 authorization portal radius-scheme bjtu
 accounting portal none
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
domain h3c
 authentication portal radius-scheme h3c
 authorization portal radius-scheme h3c
 accounting portal radius-scheme h3c
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
domain system
 authorization portal radius-scheme wang
 accounting portal radius-scheme wang
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
local-user 123
 password simple 123
 service-type lan-access
 service-type telnet
local-user h3c
 password simple h3c
 service-type telnet
 level 3
#
wlan rrm
 11a mandatory-rate 6 12 24
 11a supported-rate 9 18 36 48 54
 11b mandatory-rate 1 2
 11b supported-rate 5.5 11
 11g mandatory-rate 1 2 5.5 11
 11g supported-rate 6 9 12 18 24 36 48 54
#
wlan service-template 1 clear
 ssid web.wlan.bjtu
 bind WLAN-ESS 1
 authentication-method open-system
 service-template enable
#
wlan service-template 2 clear
 ssid yingxin.wlan.bjtu
 bind WLAN-ESS 2
 authentication-method open-system
 service-template enable
#
interface NULL0
#
interface Vlan-interface1
 ip address 10.1.154.1 255.255.255.0
#
interface Vlan-interface791
 ip address 211.71.79.3 255.255.255.192
 portal server h3c method direct
#
interface Vlan-interface792
 ip address 211.71.79.66 255.255.255.192
 portal server h3c method direct
#
interface M-GigabitEthernet1/0/1
 ip address 192.168.1.1 255.255.255.0
#
interface Ten-GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan all
#
interface WLAN-ESS1
 port access vlan 791
#
interface WLAN-ESS2
 port access vlan 792
#
wlan ap 2001 model WA2220-AG
 serial-id 210235A29E0083000070
 radio 1
  service-template 1
  service-template 2
  radio enable
 radio 2
  service-template 1
  service-template 2
  radio enable
#
wlan ap 2sushe model WA2220X-AGP
 serial-id 210235A29J0083000159
 radio 1
  service-template 2
  radio enable
 radio 2
  channel 11
  service-template 2
  radio enable
#
ip route-static 0.0.0.0 0.0.0.0 10.1.154.254
#
 snmp-agent
 snmp-agent local-engineid 800063A203000FE290A942
 snmp-agent community read public
 snmp-agent community write private
 snmp-agent sys-info version all
 snmp-agent target-host trap address udp-domain 10.1.154.1 params securityn
ame public
 snmp-agent target-host trap address udp-domain 202.112.154.60 params
securityname public
#
user-interface con 0
```

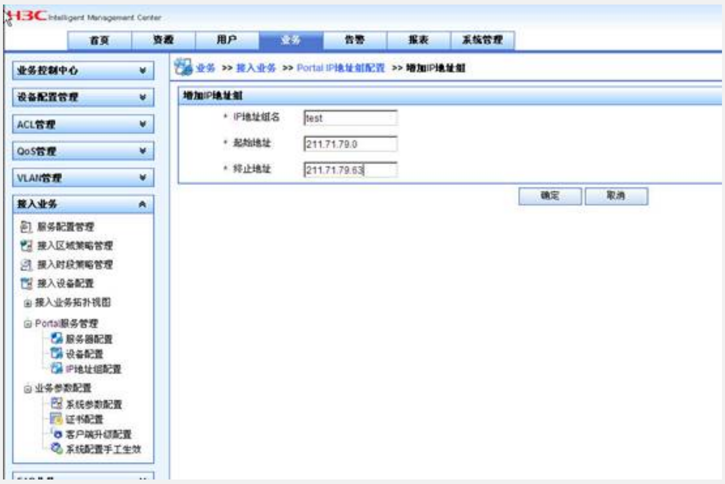
```
user-interface vty 0 4
 authentication-mode scheme
 user privilege level 3
#
return
```

四、IMC和第三方radius的配置

1、配置Portal Server.

步骤1、增加IP地址组

增加的ip地址组是指Station接入后获得的IP地址所属的网段，本例中Station获得的IP地址test池是211.71.79.0/26, 所以这里添加的ip地址组就是从211.71.79.0 到211.71.79.63。

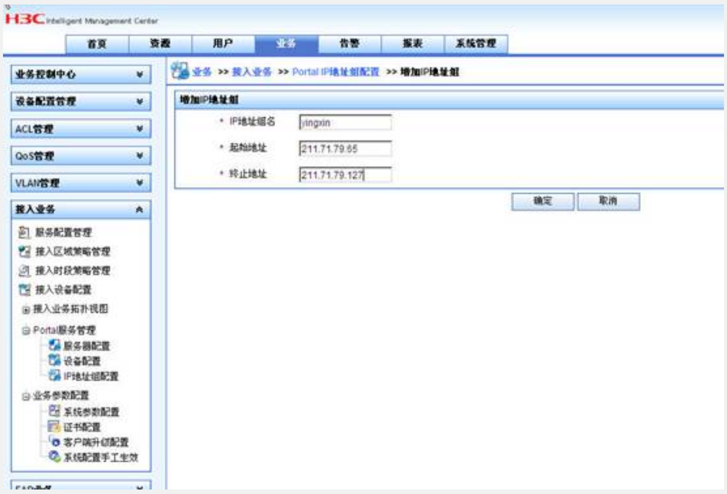


业务 >> 接入业务 >> Portal IP地址组配置 >> 增加IP地址组

增加IP地址组

- IP地址组名 test
- 起始地址 211.71.79.0
- 终止地址 211.71.79.63

本例中Station获得的IP地址yingxin池是211.71.79.65/26, 所以这里添加的ip地址组就是从211.71.79.65到211.71.79.127。



业务 >> 接入业务 >> Portal IP地址组配置 >> 增加IP地址组

增加IP地址组

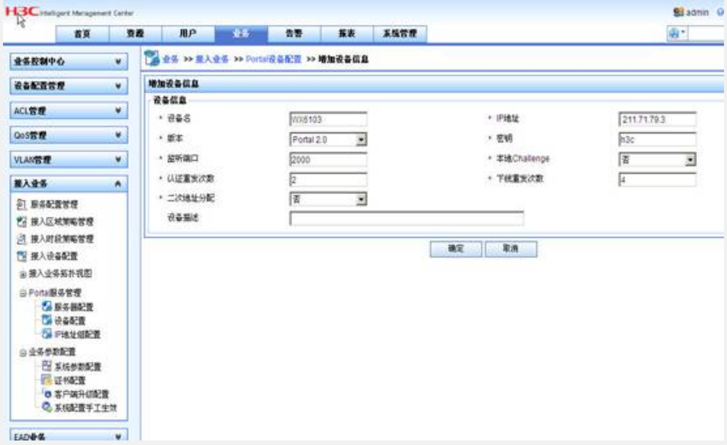
- IP地址组名 yingxin
- 起始地址 211.71.79.65
- 终止地址 211.71.79.127

步骤2、配置设备信息

配置设备信息，IP地址：Station连接的WX6103上Wlan-ESS口所属vlan的三层口IP地址。本例中为211.71.79.3和211.71.79.66。

版本：portal 2.0

密钥：WX6103上配置的portal server 的密钥。本例中为“h3c”。

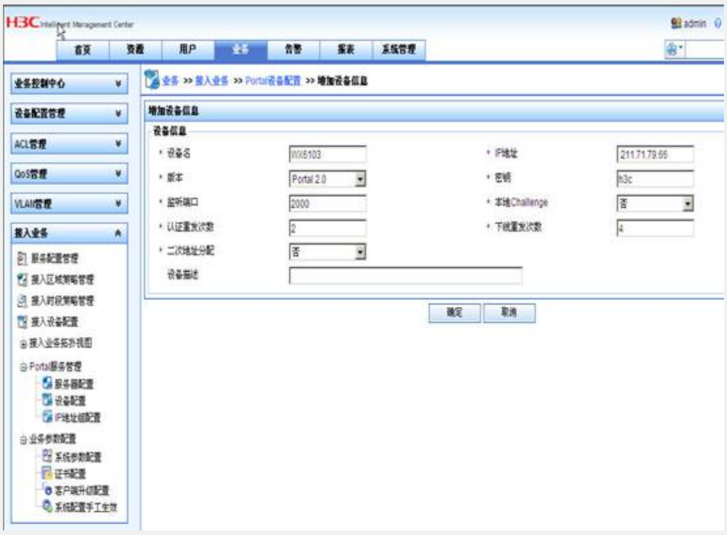


业务 >> 接入业务 >> Portal设备配置 >> 增加设备信息

增加设备信息

设备信息

* 设备名	WX6103	* IP地址	211.71.79.3
* 版本	Portal 2.0	* 密钥	h3c
* 监听端口	2000	* 本地Challenge	否
* 认证重发次数	2	* 下线重发次数	4
* 二次地址分配	否		
设备描述			



业务 >> 接入业务 >> Portal设备配置 >> 增加设备信息

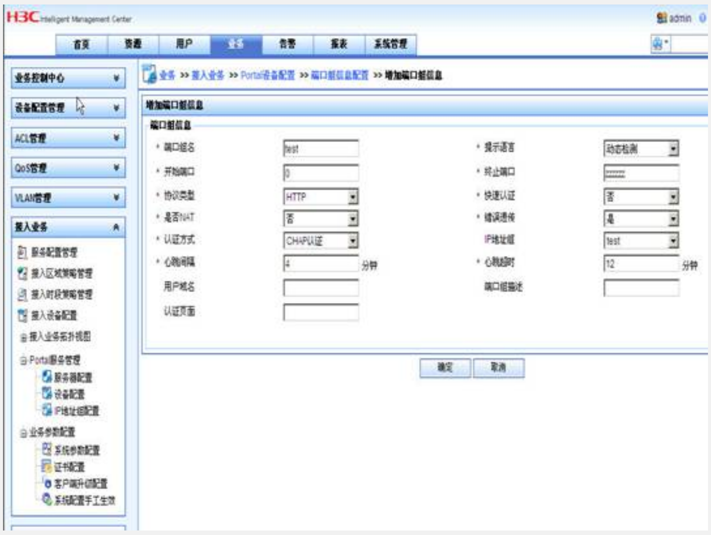
增加设备信息

设备信息

* 设备名	WX6103	* IP地址	211.71.79.65
* 版本	Portal 2.0	* 密钥	h3c
* 监听端口	2000	* 本地Challenge	否
* 认证重发次数	2	* 下线重发次数	4
* 二次地址分配	否		
设备描述			

步骤3、配置端口管理信息

主要配置端口组名和IP地址组，IP地址组选择步骤1中创建的IP地址组名。

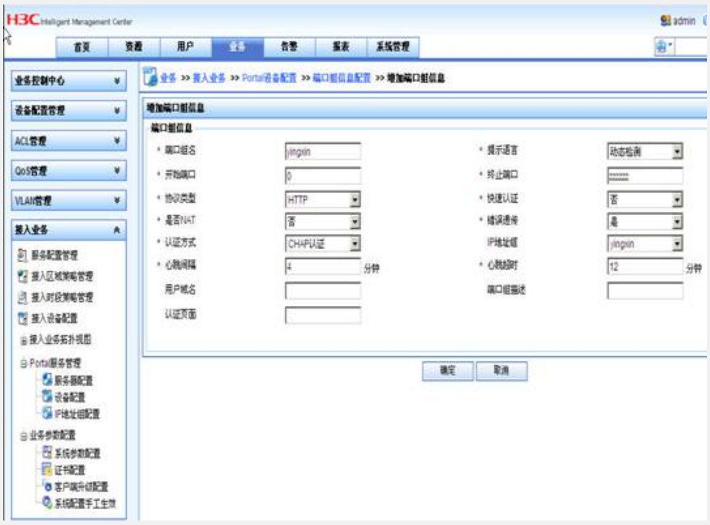


业务 >> 接入业务 >> Portal设备配置 >> 端口组信息配置 >> 增加端口组信息

增加端口组信息

端口组信息

* 端口组名	test	* 提示语言	动态检测
* 开始端口	0	* 终止端口	[illegible]
* 协议类型	HTTP	* 快速认证	否
* 是否NAT	否	* 错误透传	是
* 认证方式	CHAP认证	IP地址组	test
* 心跳间隔	4 分钟	* 心跳超时	12 分钟
用户域名		端口组描述	
认证页面			



业务 >> 接入业务 >> Portal设备配置 >> 端口组信息配置 >> 增加端口组信息

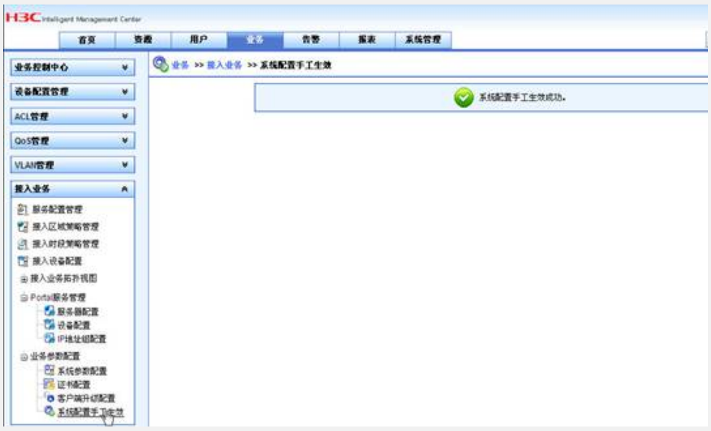
增加端口组信息

端口组信息

* 端口组名	yingxin	* 提示语言	动态检测
* 开始端口	0	* 终止端口	[illegible]
* 协议类型	HTTP	* 快速认证	否
* 是否NAT	否	* 错误透传	是
* 认证方式	CHAP认证	IP地址组	yingxin
* 心跳间隔	4 分钟	* 心跳超时	12 分钟
用户域名		端口组描述	
认证页面			

步骤4、配置生效

配置完毕后，点击系统配置手工生效。



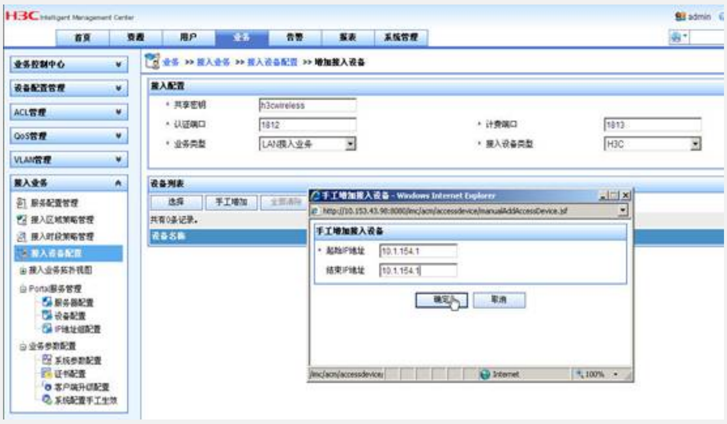
业务 >> 接入业务 >> 系统配置手工生效

系统配置手工生效成功。

2、 接入设备配置

在接入设备配置中将接入设备的IP地址加入或者保证设备的管理IP 10.1.154.1添加接入设备地址或者IP范围内10.1.154.0-10.1.154.254包含这个IP地址。

保证添加的接入设备的共享密钥与设备的配置一致，本例中为“h3cwireless”



业务 >> 接入业务 >> 接入设备配置 >> 增加接入设备

接入配置

- 共享密钥：h3cwireless
- 认证端口：1812　　计费端口：1813
- 业务类型：LAN接入业务　　接入设备类型：H3C

设备列表

共有0条记录。

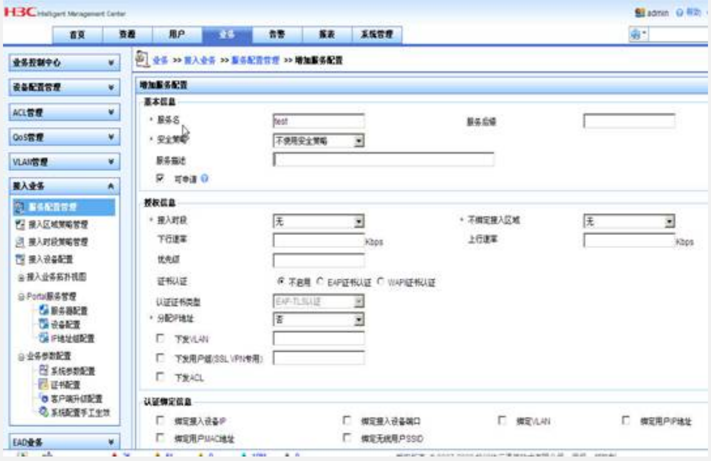
手工增加接入设备 - Windows Internet Explorer

http://10.153.43.98:8080/imc/acm/accessdevice/manualAddAccessDevice.jsf

手工增加接入设备

- 起始IP地址：10.1.154.1
- 结束IP地址：10.1.154.1

3、服务配置



业务 >> 接入业务 >> 服务配置管理 >> 增加服务配置

增加服务配置

基本信息

- 服务名：test　　服务后缀：
- 安全策略：不使用安全策略
- 服务描述：
- ☑ 可申请

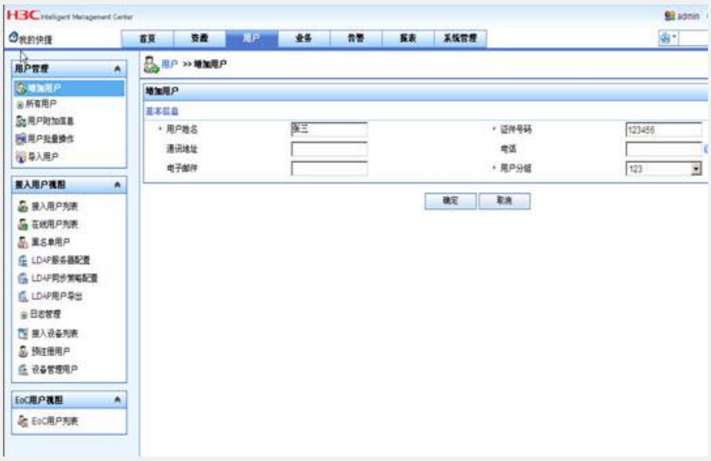
授权信息

- 接入时段：无　　不绑定接入区域：无
- 下行速率：Kbps　　上行速率：Kbps
- 优先级：
- 证书认证：● 不启用 ○ EAP证书认证 ○ WAPI证书认证
- 认证证书类型：EAP-TLS认证
- 分配IP地址：否
- □ 下发VLAN
- □ 下发用户组(SSL VPN专用)
- □ 下发ACL

认证绑定信息

□ 绑定接入设备IP　□ 绑定接入设备端口　□ 绑定VLAN　□ 绑定用户IP地址
□ 绑定用户MAC地址　□ 绑定无线用户SSID

4、创建帐户配置



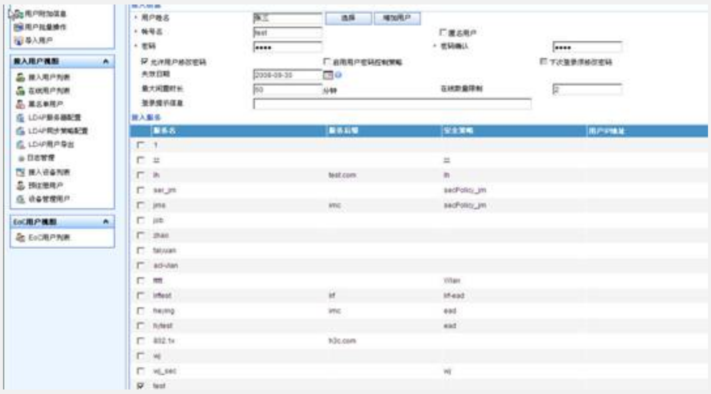
用户 >> 增加用户

增加用户

基本信息

- 用户姓名：张三　　证件号码：123456
- 通讯地址：　　电话：
- 电子邮件：　　用户分组：123

为用户帐户创建登录帐号test和yingxin,并指定相应的服务.



* 用户姓名 张三

* 帐号名 test　　☐ 匿名用户

* 密码 ****　　* 密码确认 ****

☑ 允许用户修改密码　　☐ 启用用户密码控制策略　　☐ 下次登录须修改密码

失效日期 2008-09-30

最大闲置时长 60 分钟　　在线数量限制 2

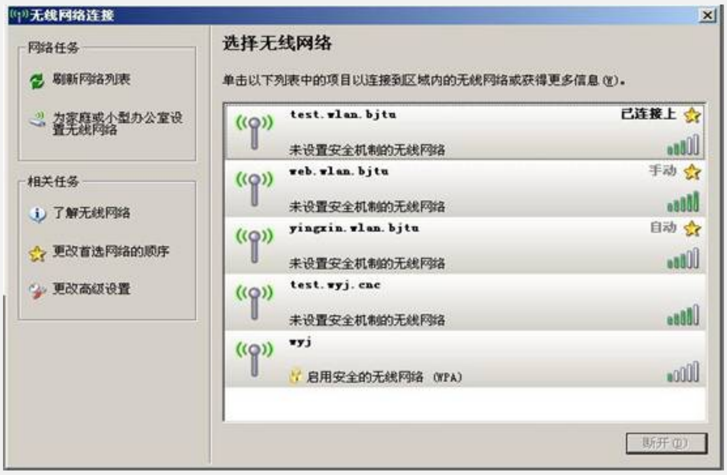
登录提示信息

接入服务

	服务名	服务后缀	安全策略	用户IP地址
☐	1			
☐	zz		zz	
☐	lh	test.com	lh	
☐	ser_jm		secPolicy_jm	
☐	jms	imc	secPolicy_jm	
☐	jlb			
☐	zhao			
☐	taiyuan			
☐	acl-vlan			
☐	ttttt		Wlan	
☐	inftest	inf	inf-ead	
☐	heying	imc	ead	
☐	hjtest		ead	
☐	802.1x	h3c.com		
☐	wj			
☐	wj_sec		wj	
☑	test			

五、验证结果

步骤1、连接SSID“test.wlan.bjtu”，自动获取211.71.79.0/26网段的地址。



test.wlan.bjtu　已连接上
未设置安全机制的无线网络

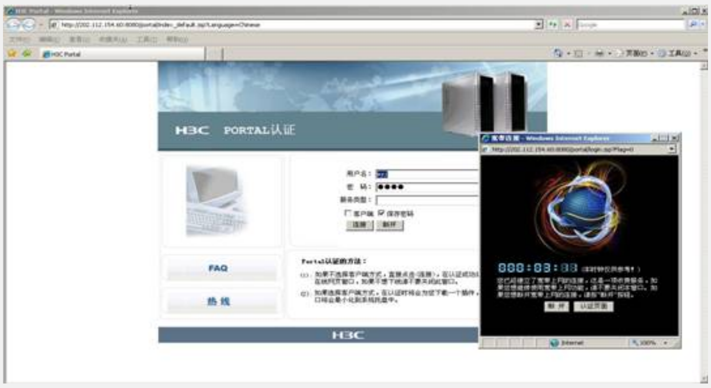
web.wlan.bjtu　手动
未设置安全机制的无线网络

yingxin.wlan.bjtu　自动
未设置安全机制的无线网络

test.wyj.cnc
未设置安全机制的无线网络

wyj
启用安全的无线网络 (WPA)

步骤2、在IE中输入任意IP地址，可重定向到http://202.112.154.60:8080/portal页面，输入用户名和密码后认证成功。此时可以访问学校的内部网络.


H3C Portal - Windows Internet Explorer
http://202.112.154.60:8080/portal/index_default.jsp?Language=Chinese
H3C Portal
H3C PORTAL认证
FAQ
热线
H3C
http://202.112.154.60:8080/portal/login.jsp?Flag=0
Internet
100%

用户名：

密　码：●●●●

服务类型：

☐ 客户端　☑ 保存密码

连接　断开

Portal认证的方法：

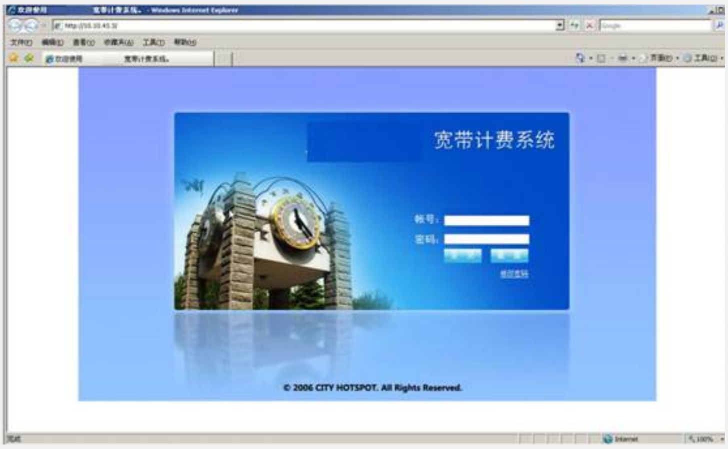
(1) 如果不选择客户端方式，直接点击《连接》，在认证成功后……

(2) 如果选择客户端方式，在认证时将会提示下载一个插件……

000:03:33

断开　认证页面

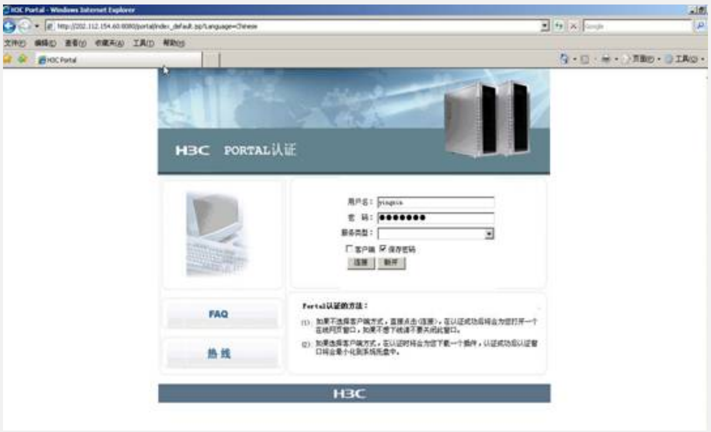
当访问公网的地址时,可以弹出和第三方radius的二次计费认证页面，输入帐号密码认证成功后，就可以访问互联网。


欢迎使用　宽带计费系统。 - Windows Internet Explorer
http://10.10.45.3/
文件(F) 编辑(E) 查看(V) 收藏夹(A) 工具(T) 帮助(H)
宽带计费系统
帐号:
密码:
修改密码
© 2006 CITY HOTSPOT. All Rights Reserved.
Internet
100%

步骤3、连接SSID“yingxin.wlan.bjtu”，自动获取211.71.79.65/26网段的地址。（不附图）

步骤4、在IE中输入任意IP地址，可重定向到http://202.112.154.60:8080/portal页面

，输入用户名和密码后认证成功。此时可以访问学校的内部网络.

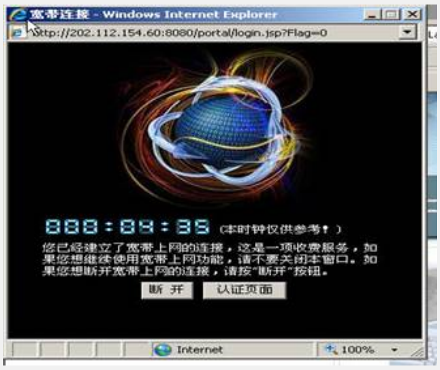

H3C Portal - Windows Internet Explorer
http://202.112.154.60:8080/portal/index_default.jsp?Language=Chinese
文件(F) 编辑(E) 查看(V) 收藏夹(A) 工具(T) 帮助(H)
H3C Portal
H3C PORTAL认证
FAQ
热线
H3C

用户名：yingxin
密 码：●●●●●●●●
服务类型：
☐ 客户端 ☑ 保存密码
连接 断开

Portal认证的方法：

(1) 如果不选择客户端方式，直接点击(连接)，在认证成功后将会为您打开一个在线网页窗口，如果不想下线请不要关闭此窗口。

(2) 如果选择客户端方式，在认证时将会为您下载一个插件，认证成功后认证窗口将会最小化到系统托盘中。


宽带连接 - Windows Internet Explorer
http://202.112.154.60:8080/portal/login.jsp?Flag=0
Internet
100%

888:84:35 (本时钟仅供参考！)

您已经建立了宽带上网的连接，这是一项收费服务，如果您想继续使用宽带上网功能，请不要关闭本窗口。如果您想断开宽带上网的连接，请按"断开"按钮。

断 开　认证页面

六、FAQ

1、默认情况下，Portal可以让广播报文和组播报文通过，所以未通过认证前Station也可以通过DHCP Server获得IP地址。

2、在未通过认证前，Station上线后应可以Ping通portal server.

3、如果通过DNS Server获取IP地址后上网，还需增加几条Portal Free规则:

[WX6103]portal free-rule 3 source any destination ip 202.112.144.236 mask 255.255.255.255

[WX6103]portal free-rule 4 source any destination ip 202.112.144.246 mask 255.255.255.255

[WX6103]portal free-rule 5 source ip 202.112.144.236 mask 255.255.255.255 destination any

[WX6103]portal free-rule 6 source ip 202.112.144.246 mask 255.255.255.255 destination any

4、AP和Station要在不同的网段，因为如果AP和Station在同一网段，在此网段启用Portal认证后会影响AP的注册。